State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

February 9, 2016

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2016-027

DATE(S) ISSUED:
02/09/2016

SUBJECT:
Vulnerability in Microsoft Windows Journal Could Allow for Remote Code Execution (MS16-013)

OVERVIEW:
A vulnerability has been discovered in Microsoft Windows Journal that could allow for remote code execution. Windows Journal is a notetaking application included in various Windows operating system installations. This vulnerability is triggered if a user opens a specially crafted Microsoft Journal (.jnt) file. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There are no reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10
- Windows Server 2008, 2008 R2
- Windows Server 2012, 2012 R2

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A memory corruption vulnerability has been discovered in Microsoft Windows Journal, which could allow for remote code execution when handling specially crafted Journal (.jnt) files. In an email attack scenario, an attacker could exploit this vulnerability by sending an email enticing a user to open a specially crafted Journal file that is attached. (CVE-2016-0038)

Successful exploitation of this vulnerability could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- If patching is not possible immediately, multiple workarounds are listed in the Microsoft reference below.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/library/security/ms16-013.aspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0038